CLAIMS

Having thus described my invention, what I claim as new and desire to secure by Letters Patent is as follows:

1. A method for encrypting a plain-text message, the method comprising:

generating a first random number;

transforming said first random number into a first pseudo random number;

further expanding a randomness of said first random number and/or said first pseudo random number into a set of pair-wise differentially-uniform pseudo random numbers;

dividing said plain-text message into a plurality of plain-text blocks;

encrypting said plain-text blocks to form a plurality of cipher-text blocks;

combining said plurality of plain-text blocks into at least one check sum; and

employing said set of pair-wise differentially-uniform pseudo random numbers, together with said first random number and/or said first pseudo random number, to embed a message integrity check in said cipher-text blocks.

2. A method as recited in claim 1, wherein the step of encrypting said plain-text blocks includes employing the said first random number, and/or said first pseudo random number, and/or said set of pair-wise differentially-uniform pseudo random numbers.

3. A method as recited in claim 1, wherein the step of employing includes pairing said first random number, and/or said first pseudo random number, and/or said set of pair-wise differentially-uniform pseudo random numbers, with said plurality of cipher-text blocks; and

combining each pair to form a plurality of output blocks.

4. A method as recited in claim 3, wherein the step of combining each pair includes performing an exclusive-or operation upon components of said each pair.

5. A method as recited in claim 1, wherein the step of encrypting includes encrypting said first random number.

6. A method as recited in claim 1, wherein the step of encrypting includes encrypting said check sum.

7. A method as recited in claim 1, wherein the step of combining includes obtaining said check sum from an exclusive-or of said plurality of plain-text blocks.

8. A method as recited in Claim 1, wherein the step of transforming said random number includes a non-cryptographic or linear operation.

9. A method as recited in Claim 1, wherein the step of transforming said random number includes a cryptographic operation.

10. A method as recited in Claim 1, wherein the said set of pair-wise differentially-uniform numbers are set of pair-wise differentially-uniform numbers in GFp.

11. A method as recited in claim 2, wherein the step of employing includes:

pairing said first random number, and/or said first pseudo random number, and/or said set of pair-wise differentially-uniform pseudo random numbers, with said plurality of plain-text blocks; and

combining each pair to form a plurality of input blocks used in said step of encrypting.

12. A method as recited in claim 11, wherein the step of combining each pair includes performing an exclusive-or operation upon components of said each pair.

13. A method for decrypting a cipher-text message, the method comprising:

dividing said cipher-text message into a plurality of cipher-text blocks;

decrypting said cipher-text blocks in forming a plurality of plain-text blocks;

transforming at least one of said plain-text blocks into a first pseudo random number;

further expanding at least one of said plain-text blocks and/or said first pseudo random number into a set of pair-wise differentially-uniform pseudo random numbers;

combining said first pseudo random number, and/or said set of pair-wise differentially-uniform pseudo random numbers, and/or said at least one plain-text block to form at least two check sums and to form a plurality of output blocks; and

comparing said at least two check sums in declaring success of a message integrity check.

14. A method as recited in claim 13, wherein the step of decrypting said cipher-text blocks includes employing said first pseudo random number, and/or said set of pair-wise differentially-uniform pseudo random numbers.

15. A method as recited in claim 13, wherein the step of combining includes:

pairing said first pseudo random number, and/or said set of pair-wise differentially-uniform pseudo random numbers, with said plurality of plain-text blocks; and

using each pair to form a plurality of output blocks and employing the output blocks to form said at least two check sums.

16. A method as recited in claim 15, wherein the step of using each pair includes performing an exclusive-or operation upon components of said each pair.

17. A method as recited in claim 15, wherein the step of forming includes:

dividing the said output blocks into at least two subsets, and

obtaining said at least two checksums from an exclusive-or of said subsets of output blocks.

18. A method as recited in Claim 13, wherein the step of transforming said plain-text blocks includes a non-cryptographic or linear operation.

19. A method as recited in Claim 13, wherein the step of transforming said plain-text blocks includes a cryptographic operation.

20. A method as recited in Claim 13, wherein the said set of pair-wise differentially-uniform numbers are set of pair-wise differentially-uniform numbers in GFp.

21. A method as recited in claim 14, wherein the step of employing includes:

pairing said first random number, and/or said first pseudo random number, and/or said set of pair-wise differentially-uniform pseudo random numbers, with said plurality of cipher-text blocks; and

combining each pair to form a plurality of input blocks used in said step of decrypting.

22. A method as recited in claim 3, wherein p is a prime number, and the step of combining each pair includes performing a modulo p addition upon components of said each pair.

23. A method as recited in claim 11, wherein p is a prime number, and the step of combining each pair includes performing a modulo p addition upon components of said each pair.

24. A method as recited in claim 15, wherein p is a prime number, and the step of using each pair includes performing a modulo p addition upon components of said each pair.

25. A method as recited in claim 21, wherein p is a prime number, and the step of combining each pair includes performing a modulo p addition upon components of said each pair.

26. An article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for causing encryption of a plain-text message, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 1.

27. An article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for causing decryption of a cipher-text message, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 13.

28. A computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing encryption of a plain-text message, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the steps of claim 1.

29. A computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing decryption of a plain-text message, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the steps of claim 13.

30. A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for encrypting a plain-text message, said method steps comprising the steps of claim 1.

31. A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for decrypting a cipher-text message, said method steps comprising the steps of claim 13.

32. A method for encryption/decryption of a plain-text message, the method comprising the steps of:

generating a first random number;

transforming said first random number into a first pseudo random number;

further expanding a randomness of said first random number and/or said first pseudo random number into a set of pair-wise differentially-uniform pseudo random numbers;

dividing the plain-text message into a plurality of plain-text blocks;

encrypting said plain-text blocks in forming a plurality of cipher-text blocks;

combining said plurality of plain-text blocks into at least one check sum; and

employing said first random number, said first pseudo random number and said set of pair-wise differentially-uniform pseudo random numbers to embed a message integrity check in said cipher-text blocks to form a cipher-text message; and

dividing said cipher-text message into a plurality of cipher-text blocks to form an encryption of said plain-text message;

decrypting said cipher-text blocks in forming a plurality of plain-text blocks;

transforming at least one of said plain-text blocks into a first pseudo random number;

further expanding at least one of said plain-text blocks and/or said first pseudo random number into a set of pair-wise differentially-uniform pseudo random numbers;

combining said first pseudo random number, and/or said set of pair-wise differentially-uniform pseudo random numbers, and/or said at least one plain-text block to form at least two check sums and to re-form the said plain-text message; and comparing said at least two check sums in declaring success of a message integrity check in decryption of said cipher-text to reform said plain-text message.

33. An apparatus to encrypt a plain-text message, the apparatus comprising:

a Randomness Generator to generate a first random number;

a Randomness Transformer to transform said first random number into a first pseudo random number;

a Pairwise Additively Uniform Sequence Generator to further expand a randomness of said first random number and/or said first pseudo random number into a set of pair-wise differentially-uniform pseudo random numbers;

an Encryptor to divide said plain-text message into a plurality of plain-text blocks, and to encrypt said plain-text blocks to form a plurality of cipher-text blocks;

a Checksum Generator to combine said plurality of plain-text blocks into at least one check sum; and

an Integrity Extractor and Checker to employ said set of pair-wise differentially-uniform pseudo random numbers, together with said first random number and/or said first pseudo random number, to embed a message integrity check in said cipher-text blocks.

34. An apparatus to decrypt a cipher-text message, the apparatus comprising:

a Decryptor to divide said cipher-text message into a plurality of cipher-text blocks, and to decrypt said cipher-text blocks in forming a plurality of plain-text blocks;

a Randomness Transformer to transform at least one of said plain-text blocks into a first pseudo random number;

a Pairwise Additively Uniform Sequence Generator to further expand at least one of said plain-text blocks and/or said first pseudo random number into a set of pair-wise differentially-uniform pseudo random numbers;

a Checksum Generator to combine said first pseudo random number, and/or said set of pair-wise differentially-uniform pseudo random numbers, and/or said at least one plain-text block to form at least two check sums and to form a plurality of output blocks; and

an Integrity Extractor and Checker to compare said at least two check sums in declaring success of a message integrity check.

35. An article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for causing encryption of a plain-text message, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 2 .

36. An article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for causing decryption of a cipher-text message, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 14.

37. A computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing encryption of a plain-text message, the computer readable program code means in said computer program

product comprising computer readable program code means for causing a computer to effect the steps of claim 2.

38. A computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing decryption of a plain-text message, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the steps of claim 14.

39. A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for encrypting a plain-text message, said method steps comprising the steps of claim 2.

40. A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for decrypting a cipher-text message, said method steps comprising the steps of claim 14.

41. A method as recited in claim 3, wherein the step of combining each pair includes performing an addition in a group upon components of said each pair.

42. A method as recited in claim 11, wherein the step of combining each pair includes performing an addition in a group upon components of said each pair

43. A method as recited in claim 15, wherein the step of using each pair includes performing an addition in a group upon components of said each pair.

44. A method as recited in claim 21, wherein the step of combining each pair includes performing an exclusive-or operation upon components of said each pair.

45. A method as recited in claim 21, wherein the step of combining each pair includes performing an addition in a group upon components of said each pair.